ガロア体とLFSR

情報数理学特別講義I 第4回

2025-11-05

今回学ぶこと

前回はガロア体を学んだ.
今回はガロア体上の各演算の回路構成について学ぶ.

係数乗算回路

係数乗算とは，$GF(2^q)$上の任意の元 x と定数 c に対して，$c \times x$ を計算することである.

$$f(x) = c \times x$$

乗算器で簡単に実装できるが，コストが高いため乗算器を使わない方法を説明する.

※今まで乗算記号を・としていましたが，これからは $\times$ とします.

係数乗算回路

定数 c を原始元のべき α^i とし，引数である a を多項式表現としたとき，
乗算 $c \times a$ は次のように書ける．

$$\begin{aligned}
\alpha^i \times a &= \alpha^i \times \left(a_0 + a_1\alpha + \cdots + a_{q-1}\alpha^{q-1}\right) \\
&= a_0\alpha^i + a_1\alpha^{i+1} + \cdots + a_{q-1}\alpha^{i+q-1} \\
&= \left(\alpha^i, \alpha^{i+1}, \ldots, \alpha^{i+q-1}\right) \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{q-1} \end{pmatrix}
\end{aligned}$$

α^i はベクトル表現で長さ q のバイナリベクトルであることから，係数乗算は $q \times q$ の
バイナリ行列との積で計算ができる．乗算器が $O(q^3)$ の計算量だったのに対して，バイナリ行列
の積は $O(q^2)$.

練習問題(6分)

$p(x) = 1 + x^2 + x^5$ で定義される $GF(2^5)$ において
(1) $p(x)$ の根(原始元) α の乗算に相当するバイナリ行列(係数乗算の行列) A を求めよ.
(2) α^2 の乗算に相当するバイナリ行列 A^2 を求めよ.
(3) (1)で求めた A を用いて $A \times A$ を計算せよ.

参考：

$$\alpha^i \times a = \alpha^i \times \left(a_0 + a_1\alpha + \cdots + a_{q-1}\alpha^{q-1}\right)$$

$$= \left(\alpha^i, \alpha^{i+1}, \ldots, \alpha^{i+q-1}\right) \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{q-1} \end{pmatrix}$$

2乗回路

$GF(2^q)$上の任意の元 x の2乗

$$f(x) = x^2$$

を計算する回路を実装するにはどうすればよいか.

ナイーブな実装は乗算回路を使う方法だが，乗算回路はコストが高いので好ましくない.
係数乗算と同様に，2元拡大体 $GF(2^q)$ の場合には効率的な実装方法がある.

$GF(2^q)$ の2乗回路

(重要な性質) $GF(2^q)$ の元 α の多項式には以下が成り立つ.

$$f(\alpha)^2 = f(\alpha^2)$$

つまり, $GF(2^q)$ の元（多項式表現）$a(\alpha)$ の2乗は次のように計算することができる.

$$a(\alpha)^2 = a(\alpha^2) = a_0 + a_1\alpha^2 + \cdots + a_{q-1}\alpha^{2(q-1)}$$

$GF(2^q)$ の2乗回路は $q \times q$ バイナリ行列との積となる

$$a(\alpha)^2 = a(\alpha^2) = a_0 + a_1\alpha^2 + \cdots + a_{q-1}\alpha^{2(q-1)}$$

はベクトル表現を用いると

$$a^2 = \left(1, \alpha^2, \ldots, \alpha^{2(q-1)}\right) \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{q-1} \end{pmatrix}$$

とかける．$\left(1, \alpha^2, \ldots, \alpha^{2(q-1)}\right)$ の各要素は長さ q のバイナリベクトルであることから，2乗の計算は $q \times q$ のバイナリ行列との積で計算ができる．計算量は $O(q^2)$ となり，$O(q^3)$ の乗算よりも少ない計算量で計算が実行できる．なお，a^4 は $\left(a^2\right)^2$ であるので，同様にバイナリ行列積で計算できる．つまり，a^{2^s} **のべきの計算は全てバイナリ行列積で計算できる**．

練習問題2(5分)

$p(x) = 1 + x^2 + x^5$ で定義される $GF(2^5)$ の2乗，4乗演算となるバイナリ行列をそれぞれ示せ.

参考：a^2のベクトル表現

$$a^2 = \left(1, \alpha^2, \ldots, \alpha^{2(q-1)}\right) \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{q-1} \end{pmatrix}$$

逆元（割り算）の計算

$a \in GF(2^q)$ を入力し $a^{-1} \in GF(2^q)$ を出力する逆元計算は2通りの方法で実現できる.

- 乗算による方法
- テーブル参照による方法

逆元計算：乗算による方法

$a^{-1} = a^{2^q-2}$ より(*)，次のように 2^s 乗の累積で計算できる.

$$a^{-1} = a^{2^q-2} = a^2 \times a^4 \cdots a^{2^{q-1}}$$

2^s 乗は通常の乗算よりも計算コストが少ないため，2^s 乗の累積で計算することで，乗算のみを繰り返すよりも逆元計算の計算コストを抑えることができる.
しかしながら，乗算を $q-2$ 回必要になるため，逆元の計算コストは大きい.

(*) $a^{2^q-1} = 1$ であるため．この性質は原始元に限らず，全ての非零元に対して成り立つ.

逆元計算：テーブル参照による方法

高速性が要求されるアプリケーションでは，乗算を複数回実施することが難しいため，
元 $a \in GF(2^q)$ を引数にとり，その逆元 $a^{-1} \in GF(2^q)$ を返す要素数が 2^q 個のテーブルを参照して逆元を求める回路が実装されることが多い．

- ゼロ元の逆元を計算することはないが，万が一ゼロ元が入力された際に異常な入力であることを示すような値を返すようにしておくことがある．

例：$GF(2^4)$の逆元テーブル，$p(x) = 1 + x + x^4$.

Elements (vec. repr.)	Inversion	Elements (vec. repr.)	Inversion
(0,0,0,0)	no inversion	(0,0,0,1)	(1,1,1,1)
(1,0,0,0)	(1,0,0,0)	(1,0,0,1)	(0,1,0,0)
(0,1,0,0)	(1,0,0,1)	(0,1,0,1)	(0,0,1,1)
(1,1,0,0)	(0,1,1,1)	(1,1,0,1)	(1,0,1,0)
(0,0,1,0)	(1,0,1,1)	(0,0,1,1)	(0,1,0,1)
(1,0,1,0)	(1,1,0,1)	(1,0,1,1)	(0,0,1,0)
(0,1,1,0)	(1,1,1,0)	(0,1,1,1)	(1,1,0,0)
(1,1,1,0)	(0,1,1,0)	(1,1,1,1)	(0,0,0,1)

一般にテーブル参照による実装のほうが逆元を得るまでの計算時間は短いものの，2^q 個の要素を持つテーブルを保持しなくてはならないため，q に対して指数関数的に回路規模が増大するといった問題がある.

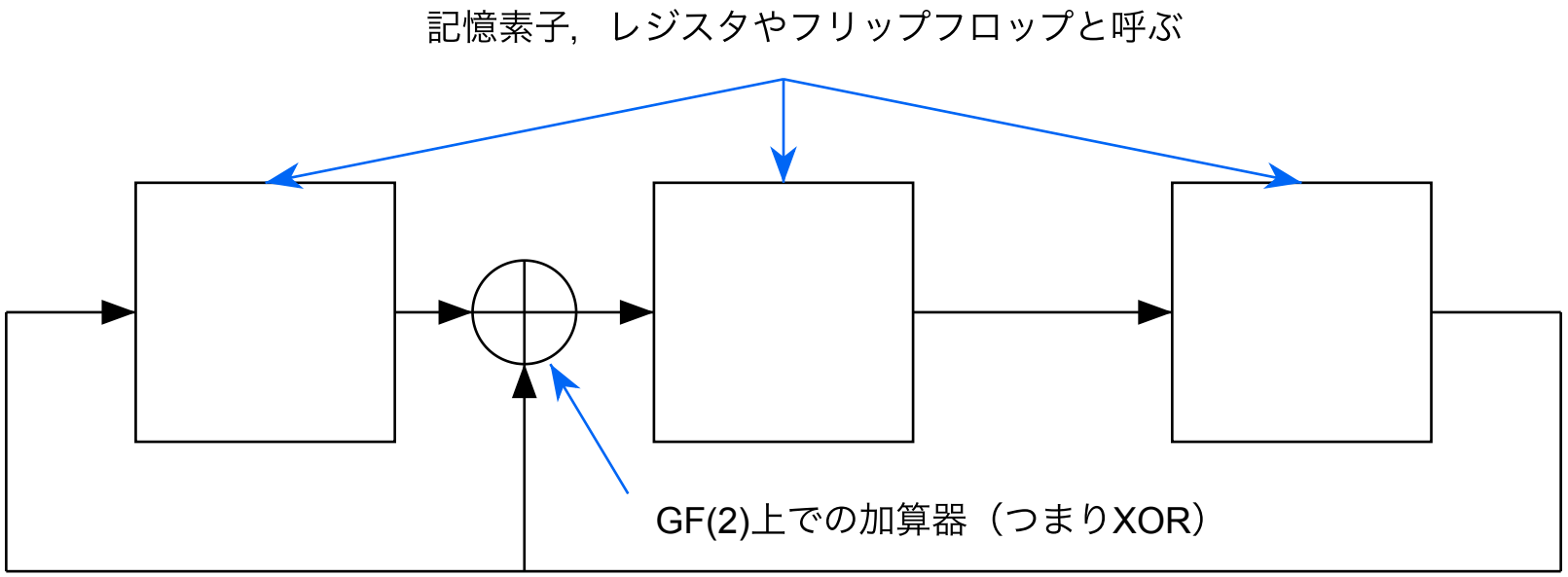
練習問題3(3分)

先のテーブルの逆元の組が正しいか，多項式表現の乗算で確かめてみよう.
$\alpha^4 = (1,1,0,0)$，$\alpha^{-4} = (0,1,1,1)$ より，
多項式表現はそれぞれ $\alpha^4 = 1 + \alpha$，$\alpha^{-4} = \alpha + \alpha^2 + \alpha^3$.

$\alpha^4 \times \alpha^{-4}$ を計算してみよ.
ただし，$GF(2^4)$ を定義する原始多項式は $p(x) = 1 + x + x^4$ とする.

ガロア体と線形帰還シフトレジスタ

ガロア体 $GF(2^q)$ の元 α^i は線形帰還シフトレジスタ(Linear Feedback Shift Register: LFSR)で生成できる.

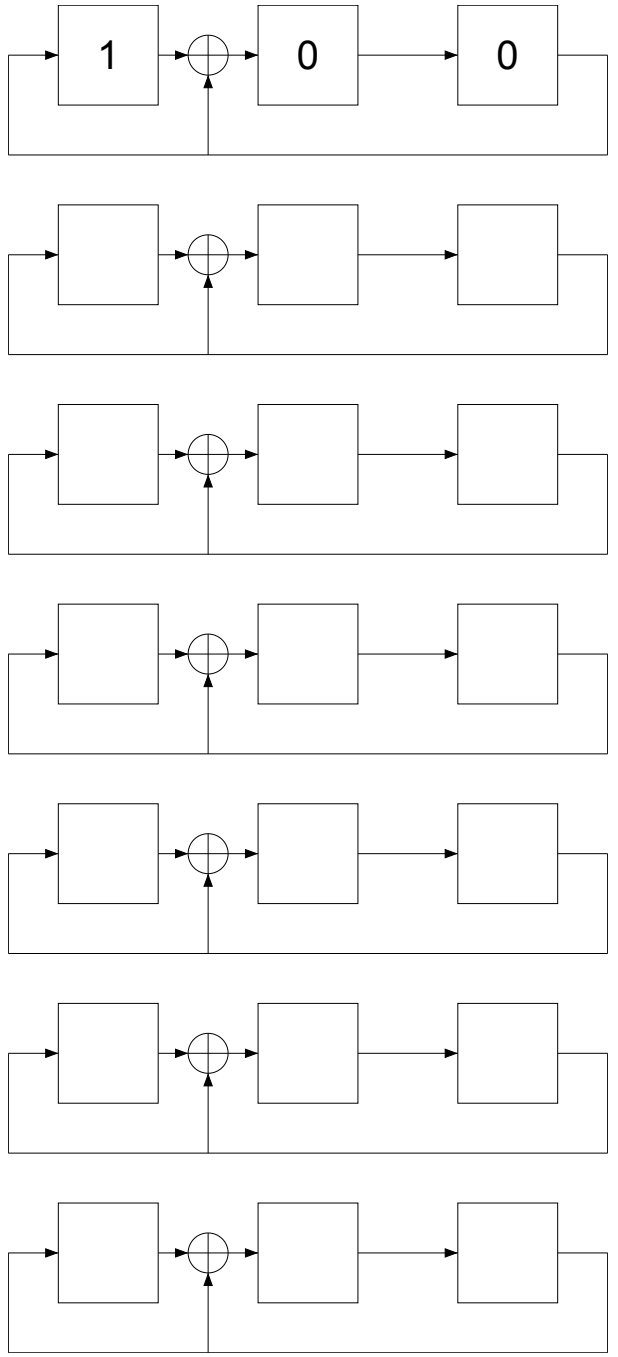


上図は $p(x) = 1 + x + x^3$ で構成された $GF(2^3)$ の元を生成するLFSR

LFSRによる元の生成例

Power repr.	Polynomial repr.	Vector repr.
0	0	$(0,0,0)^{\mathrm{T}}$
α^0	1	$(1,0,0)^{\mathrm{T}}$
α^1	α	$(0,1,0)^{\mathrm{T}}$
α^2	α^2	$(0,0,1)^{\mathrm{T}}$
α^3	$1+\alpha$	$(1,1,0)^{\mathrm{T}}$
α^4	$\alpha+\alpha^2$	$(0,1,1)^{\mathrm{T}}$
α^5	$1+\alpha+\alpha^2$	$(1,1,1)^{\mathrm{T}}$
α^6	$1+\alpha^2$	$(1,0,1)^{\mathrm{T}}$

$p(x)=1+x+x^3$ で構成された $GF(2^3)$ の元（上記の表）がLFSRで生成される様子をデモンストレーションする.



練習問題4(5分)

$p(x) = 1 + x^2 + x^3$で構成された $GF(2^3)$ に対応するLFSRを構成し,
初期値を $(1, 0, 0)$ にして動作させたときに非零元が全て出力されることを確かめよ.

Juliaによるプログラム実装例

```
function lfsr(r)      # r: レジスタの内容 Integerを想定
    rr = r << 1       # レジスタの内容をシフト
    if rr >= 8        # 1がフィードバックされる場合（最上位のレジスタが1だった時）
        rr ⊻= 0b1101 # フィードバックされる最上位の1を打ち消すと共にフィードバック
    end               # ⊻ は XOR演算子
    return rr
end

r = 1 # (1,0,0)
julia> r = lfsr(r)
2 # (0,1,0)
julia> r = lfsr(r)
4 # (0,0,1)
julia> r = lfsr(r)
5 # (1,0,1)
julia> r = lfsr(r)
7 # (1,1,1)
```

Juliaによるプログラム実装例（続き）

```
r = 1 # (1,0,0)
julia> r = lfsr(r)
2 # (0,1,0)
julia> r = lfsr(r)
4 # (0,0,1)
julia> r = lfsr(r)
5 # (1,0,1)
julia> r = lfsr(r)
7 # (1,1,1)
julia> r = lfsr(r)
3 # (1,1,0)
julia> r = lfsr(r)
6 # (0,1,1)
julia> r = lfsr(r)
1 # (1,0,0)
```

Power repr.	Polynomial repr.	Vector repr.
0	0	$(0,0,0)^{\mathrm{T}}$
α^0	1	$(1,0,0)^{\mathrm{T}}$
α^1	α	$(0,1,0)^{\mathrm{T}}$
α^2	α^2	$(0,0,1)^{\mathrm{T}}$
α^3	$1+\alpha^2$	$(1,0,1)^{\mathrm{T}}$
α^4	$1+\alpha+\alpha^2$	$(1,1,1)^{\mathrm{T}}$
α^5	$1+\alpha$	$(1,1,0)^{\mathrm{T}}$
α^6	$\alpha+\alpha^2$	$(0,1,1)^{\mathrm{T}}$

原始多項式で結線したLFSRは疑似乱数生成器

- 疑似乱数とは，ランダムに0と1が生成されるように見えるが，実際には決定的なアルゴリズムによって生成される数列のこと．初期値が同じであれば同じ数列が生成される．
- LFSRのレジスタ（たとえば最上位ビット）からビットを出力することで，疑似乱数列を生成することができる．
- 原始多項式で結線したLFSRから出力される周期が $2^q - 1$ の2元系列は Maximum-length sequence (M系列) と呼ばれる．良好な自己相関特性を持つことからレーダーや同期用信号系列として用いられる．
- 長さ $2^q - 1$ のM系列は 2^{q-1} 個の1と $2^{q-1} - 1$ 個の0を持つ．

周期15 のM系列の自己相関特性

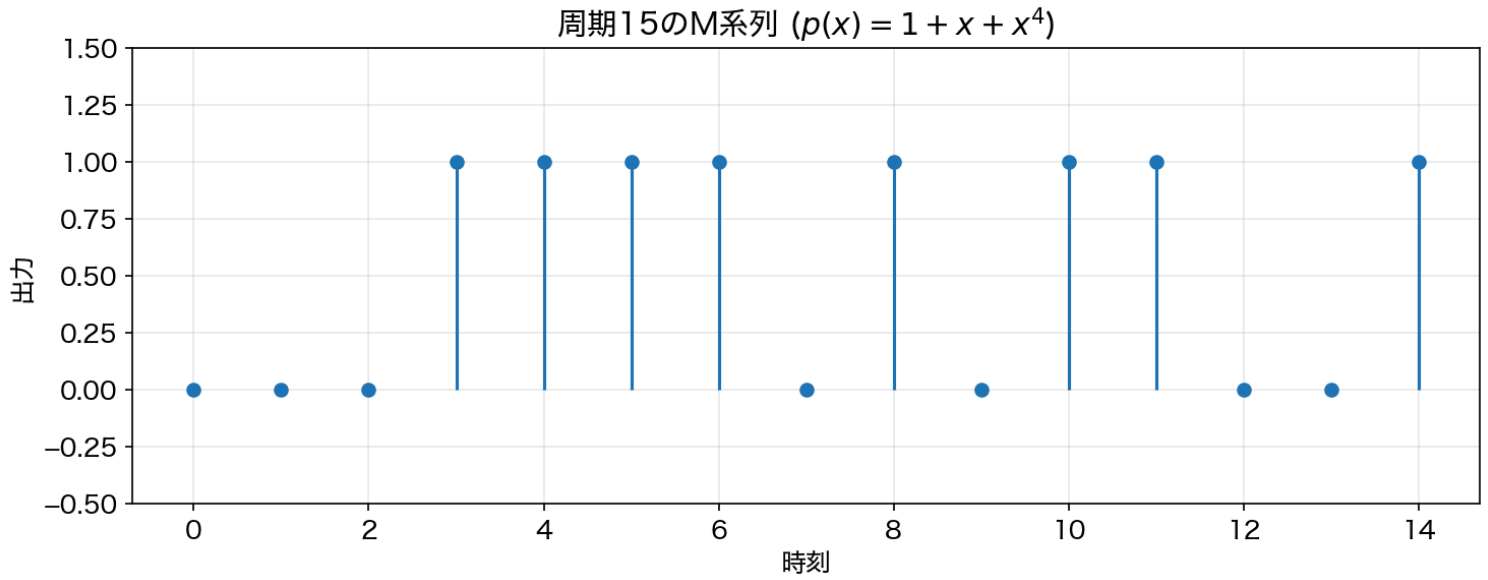
原始多項式 $p(x) = 1 + x + x^4$ で生成される周期15のM系列の自己相関特性を考える.

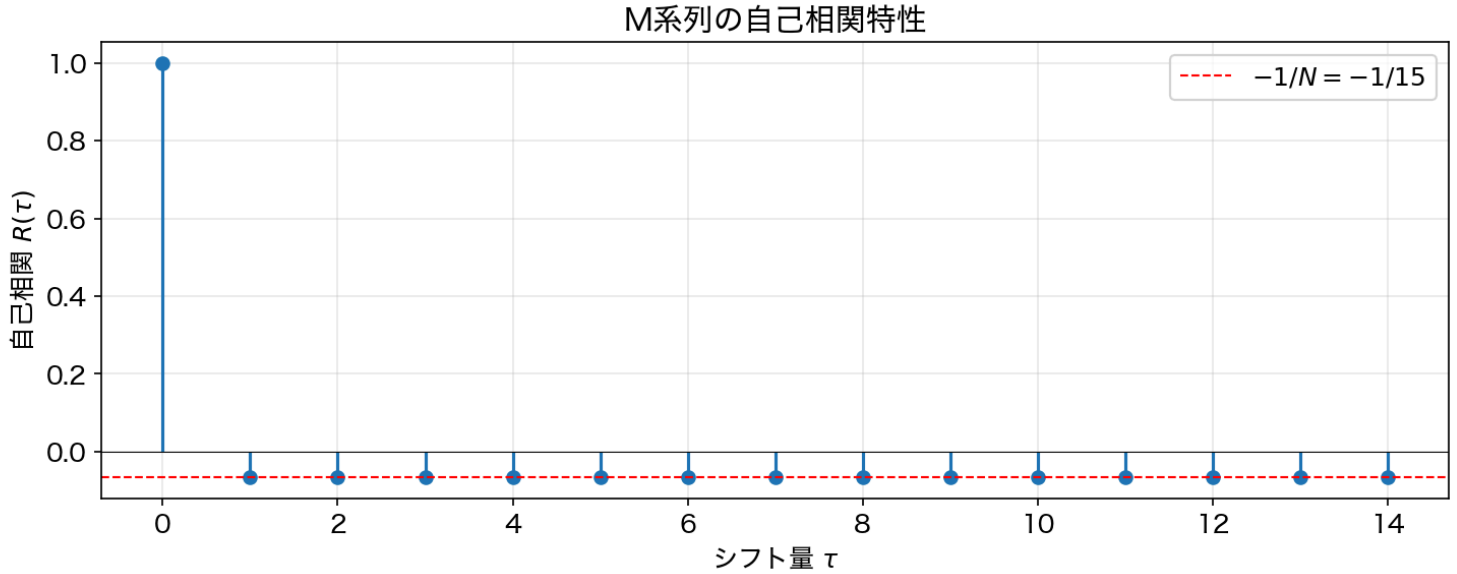
M系列 $s(t)$ の自己相関関数 $R(\tau)$ は次のように定義される.

$$R(\tau) = \frac{1}{N} \sum_{t=0}^{N-1} s(t) \cdot s(t+\tau)$$

ここで，N は系列の周期（この場合 $N = 15$），$s(t) \in \{-1, 1\}$ はBPSK変調された系列（0を-1に，1を1に変換）である.

周期15のM系列の場合，$\tau \neq 0$ のとき $R(\tau) = -\frac{1}{15} \approx -0.067$ となる.


周期15のM系列 ($p(x) = 1 + x + x^4$)
出力
時刻
1.50
1.25
1.00
0.75
0.50
0.25
0.00
−0.25
−0.50
0
2
4
6
8
10
12
14


M系列の自己相関特性
自己相関 $R(\tau)$
シフト量 τ
$-1/N = -1/15$
1.0
0.8
0.6
0.4
0.2
0.0
0
2
4
6
8
10
12
14

演習

課題：$p(x) = 1 + x^2 + x^5$ で定義される $GF(2^5)$ において，$p(x)$ の根(原始元)を α とするとき，以下の問に答えよ.
(1) α^5 のコンパニオン行列 A^5 を求めよ.
(2) α^{10} のコンパニオン行列 A^{10} を求めよ.
(3) $\alpha^5 \times a$ を計算せよ．ただし $a = (1, 0, 0, 1, 0)^{\mathrm{T}}$ とする.
なお解はベクトルもしくは多項式表現で答えること.
(4) a をべき表現 α^i としたときの，i を答えよ．なお，i をどのように導出したかその導出方法についても述べること.